Tofino Security

White Paper

Version 1.0
Published December 20, 2012

Understanding Deep Packet Inspection for SCADA Security

Contents

Authors

Eric Byres, P. Eng., ISA Fellow,
CTO and VP of Engineering, Tofino Security.
eric.byres@belden.com
www.tofinosecurity.com

Executive Summary

The world's manufacturing, energy and transportation infrastructures are currently facing a serious security crisis. These critical systems are largely based on legacy SCADA and Industrial Control System (ICS) products and protocols. Many of these products are decades old and were never designed with security in mind.

Yet industry has also embraced new network technologies like Ethernet and TCP/IP, which have enabled instant access to data throughout the organization, including the plant floor. While this interlinking improves efficiency, it also significantly increases the exposure of these control systems to external forces such as worms, viruses and hackers.

Given the 20 year life cycle common for industrial systems, it will be many years before more secure ICS and SCADA devices and protocols are in widespread use. This leaves millions of legacy control systems open to attack from even the most inexperienced hacker. If a hacker or worm can get any control system access, it can exploit the protocol to disable or destroy most industrial controllers.

The good news is that there is an effective and easy-to-deploy solution to this security crisis. Using an advanced technology called "Deep Packet Inspection" (DPI), SCADA-aware firewalls can offer fine-grained control of control system traffic. This white paper explains what DPI is and how it compares to traditional IT firewalls. It then outlines how engineers can use DPI to block the malicious or inappropriate traffic, while avoiding needless reliability impacts on the control system. A case history illustrates how a seaway management company used Modbus DPI firewalls to secure a mission critical canal system.

The Need for Better Security Technology

Over the past decade, industry has embraced network technologies like Ethernet and TCP/IP for SCADA and process control systems. This has enabled companies to operate cost effectively and implement more agile business practices through instant access to data throughout the organization, including the plant floor.

While companies reap the benefits of these new technologies, many are also discovering the inherent dangers that result from making control systems more accessible to a wider range of users. Linking corporate systems together to provide access to managers, customers and suppliers significantly increases the exposure of these systems to external forces such as worms, viruses and hackers.

To make matters worse, network protocols used by SCADA and Industrial Control Systems (ICS) were never designed with security in mind. If they offer any capability to restrict what users can do over the network, it is primitive and easy to subvert. If an individual is allowed to read data from a controller, then they can also shut down or reprogram the controller.

These issues are likely to remain with us for at least the next decade. Industrial control systems are rarely replaced; their useful lives may be 10, 20 or more years. Similarly, the security limitations of the SCADA and ICS protocols cannot be addressed through patches, as their functionality is defined in established standards that take years to change.

It will be years before newer, more secure ICS and SCADA devices are in widespread use. This leaves millions of legacy control systems open to attack from even the most inexperienced hacker. If a hacker or worm can get any control system access, it can exploit the protocol to disable or destroy most industrial controllers.

The good news is that there is a solution to this problem. It is easy to use. It doesn't require the complete replacement of billions of dollars of existing SCADA and ICS equipment. And it is very effective.

The solution is a technology called "Deep Packet Inspection" (DPI) and it offers fine-grained control of SCADA network traffic. This white paper explains what DPI is and how it is being used to secure critical SCADA systems throughout the world.

Some Firewall Basics

To understand how DPI works, it is important to understand how the traditional IT firewall works. A firewall is a device that monitors and controls traffic flowing in or between networks. It starts by intercepting the traffic passing through it and comparing each message to a predefined set of rules (called Access Control Lists or ACLs). Any messages that do not match the ACLs are prevented from passing through the firewall.

The traditional firewall allows ACLs to check three primary fields in a message[1]:

1. The address of the computer sending the message (i.e. the Source IP Address),
2. The address of the computer receiving the message (i.e. the Destination IP Address),
3. The application layer protocol contained by the IP message, as indicated in the destination port number field (i.e. the Destination Port).

The source and destination address checks are easy to understand. These restrict traffic flows to specific computers, based on their IP addresses. As long as the addresses remain the same, the firewall can control which computers can interact.

The destination port number needs a bit more explanation. These ports are not physical ports like an Ethernet or USB port, but instead are special numbers embedded in every TCP or UDP message. They are used to identify the application protocol being carried in the message. For example, the Modbus/TCP protocol uses port 502, while the web protocol, HTTP, uses port 80. These numbers are registered under the Internet Assigned Numbers Authority (IANA) and are rarely ever changed.

To put this all together, imagine you only want to allow web traffic (i.e. HTTP traffic) from a client at IP address 192.168.1.10 to a web server with an address of 192.168.1.20. Then you would write an ACL rule something like:

```
"Allow Src=192.168.1.10 Dst=192.168.1.20 Port=HTTP"
```

You would load this ACL in the firewall and as long as all three criteria were met, the message would be allowed through.

Or perhaps you want to block all Modbus traffic from passing through the firewall. You would simply define a rule that blocks all packets containing 502 in the destination port field.

Seems simple, doesn't it?

The Problem: SCADA/ICS Protocols Have No Granularity

The problem with this simple scheme is that it is very black and white. Using a traditional IT firewall, one can either allow a certain protocol or block it. Fine-grained control of the protocol is impossible.

This is an issue because the SCADA ICS protocols themselves have no granularity. From the perspective of the port number, a data read message looks EXACTLY like a firmware update message. If you allow data read messages, from an HMI to a PLC, to pass through a traditional

[1] Technically speaking, there are other fields that the typical IT firewall can check, but these three fields account for 99% of all firewall rules.

firewall, you are also allowing programming messages to pass through. This is a serious security issue.

For example, in the spring of 2009 a US Government agency produced a report for major energy companies that stated:

> *"A vulnerability has been identified and verified within the firmware upgrade process used in control systems deployed in Critical Infrastructure and Key Resources (CIKR)... development of a mitigation plan is required to protect the installed customer base and the CIKR of the nation. Firmware Vulnerability Mitigation Steps [includes] blocking network firmware upgrades with appropriate firewall rules."*

Unfortunately, the IT firewalls available on the market could not differentiate between the different SCADA commands. As a result, *"blocking network firmware upgrades with appropriate firewall rules"* results in the blocking of **all** SCADA traffic. Since the reliable flow of SCADA traffic is critical to the average industrial facility, most engineers opted to let everything pass and take their chances with security.

The Solution: Deep Packet Inspection

Clearly the firewall needs to dig deeper into the protocols to understand exactly what the protocol is being used for. And that is exactly what Deep Packet Inspection does. After the traditional firewall rules are applied, the firewall inspects the content contained in the TCP/IP messages and applies more detailed rules. It is designed to understand the specific SCADA protocols and then apply filters on fields and values that matter to control systems. Depending on the protocol, these fields might include commands (such as Register Read vs. Register Write), objects (such as a Motor Object), services (get vs. set) and PLC address ranges.

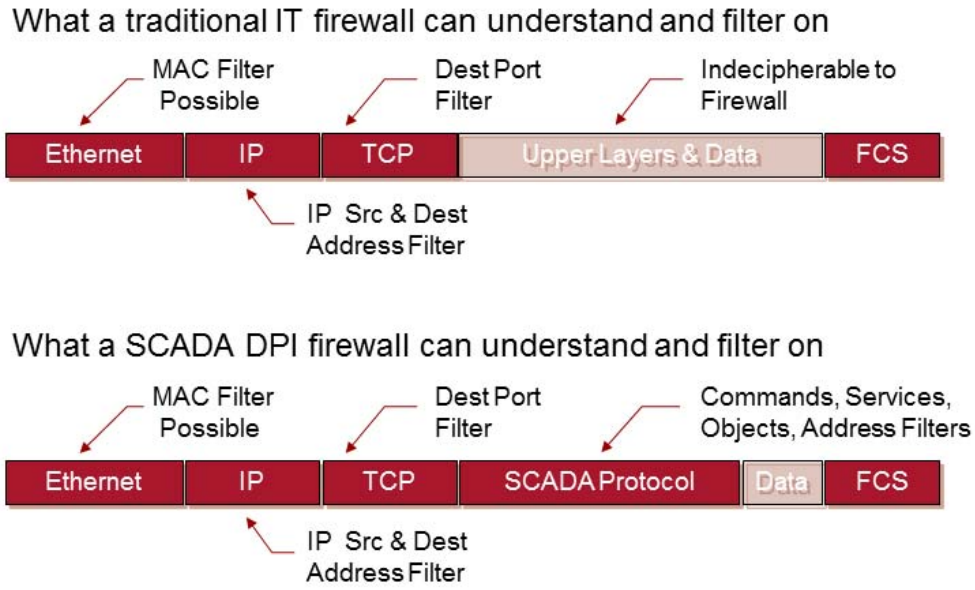


Figure 1: Comparing filtering options in a traditional firewall and a DPI Firewall. A traditional firewall cannot understand the SCADA protocol and thus can only allow or deny all SCADA messages as a group.

For example, a Modbus DPI firewall (such as the Honeywell Modbus Read-only Firewall or the Schneider ConneXium Tofino Firewall) determines if the Modbus message contains a read or a write command and then drops all write messages. Good DPI firewalls can also "sanity check" traffic for strangely formatted messages or unusual behaviours (such as 10,000 reply messages in response to a single request message). These sorts of abnormal messages can indicate traffic created by a hacker trying to crash a PLC and need to be blocked.

DPI SCADA Security in the Real World

Fine-grained control of SCADA/ICS traffic can significantly improve the security and reliability of a system. For example, consider the real world case of a seaway management company. It uses Schneider PLCs at all its control locks and bridges to ensure the safety of ship and vehicle traffic. Making sure that these PLCs are not tampered with is critical for the safety of both the ships and the public traveling over bridges at the locks.

The problem this company faced was that a number of operations computers needed to continuously access PLCs for data. However only special control computers should be permitted to send commands and impact the operation of equipment. Traditional password or IT firewall solutions were not considered secure, because they didn't offer the fine-grained control needed.

The solution was to use Modbus DPI firewalls to control all traffic to the PLC. Only Modbus Read messages were allowed to reach the PLCs (except for a few high security computers). All remote Modbus programming commands were blocked so that programming was restricted to onsite engineers. A total of 54 DPI firewalls were installed in 24 locations and the system has run without incident since late 2008.

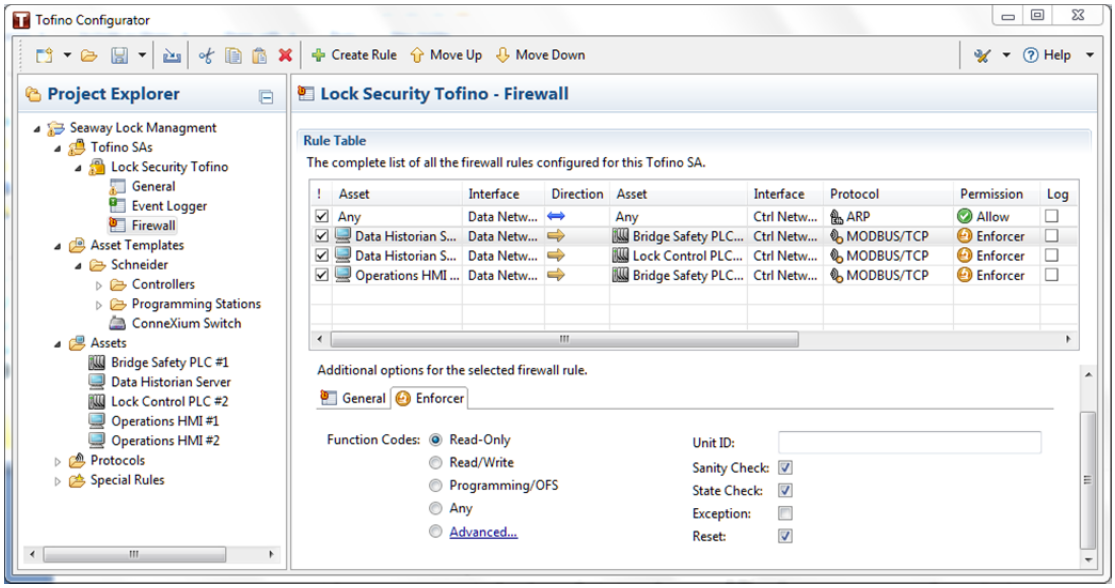


Figure 2: Firewall rules restricting Modbus traffic between the Data Historian and PLCs to Read-only commands. Other filters such as "Sanity-Check" and "State Check" ensure that all traffic match the Modbus specifications.

Why New Malware Demands DPI Technology

Five years ago, DPI was considered a nice-to-have capability. Now thanks to the current generation of worms like Stuxnet, Duqu and Conficker, it is a must-have technology if you want a secure ICS or SCADA system.

Today's malware designers know that firewalls and intrusion detection systems will spot the use of an unusual protocol instantly. They know that if the protocols on a network are normally HTTP (i.e. web browsing), Modbus and MS-SQL (i.e. database queries) then the sudden appearance of a new protocol will put the smart system administrator on his or her guard.

Thus worm designers work to stay under the radar by hiding their network traffic inside protocols that are already common on the network they are attacking. For example, many worms now hide their outbound communications in what appear to be normal HTTP messages.

Stuxnet is a particularly good example of this covert use of otherwise innocent protocols. It made heavy use of a protocol called Remote Procedure Call (RPC) for both infecting new victims and for peer-to-peer (P2P) communications between infected machines.

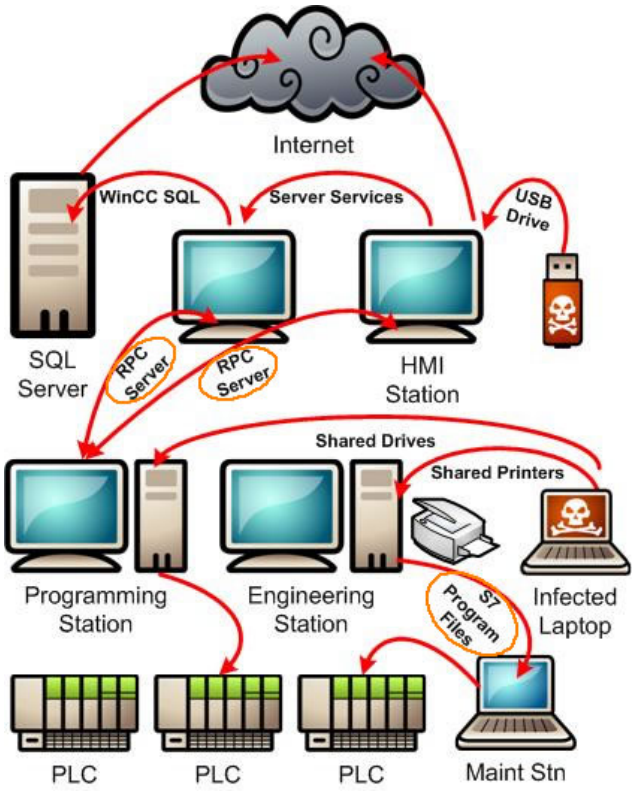


Figure 3: Stuxnet spread many ways, including using the RPC protocol as a vector. Deep Packet Inspection could have detected this non-standard use of the protocol and restricted some of the ways the worm spread.

RPC is an ideal protocol for SCADA and ICS attacks because it is used for so many legitimate purposes in modern control systems. For example, the dominant industrial integration technology, OPC Classic, is based on DCOM and this in turn requires that RPC traffic be allowed.

Furthermore, control system servers and workstations are routinely configured to share files or printers using the Microsoft SMB protocol, which also runs on top of RPC. Perhaps most relevant in this example, all Siemens PCS 7 control systems make extensive use of a proprietary messaging technology that travels over RPC. If you were an administrator

watching network traffic on a Stuxnet infected network, all you would see was a little more RPC traffic than usual, hardly a cause for alarm.

Even if you suspected something was wrong, you would be thwarted if all you had was a normal firewall. The simple blocking of all RPC traffic would likely result in a self-induced denial of service for your entire factory. Without tools to inspect the content of RPC messages and block suspicious traffic (i.e. Deep Packet Inspection), you would be unable to stop the malware.

Deep Packet Inspection Provides Robust Security for SCADA

DPI technology is a very powerful tool in the security tool box. It allows the engineer to block the malicious or inappropriate SCADA/ICS traffic, yet avoid needless impact on the control system. Without it, the designers of modern worms clearly have the upper hand. In order to stay ahead of today's advanced threats, DPI capability has become a must-have in all industrial firewalls.

References

How Stuxnet Spreads

https://www.tofinosecurity.com/how-stuxnet-spreads

PLC Security Risk: Controller Operating Systems

https://www.tofinosecurity.com/blog/plc-security-risk-controller-operating-systems

Tofino Enforcer Revolutionizes Modbus TCP/IP Security

http://www.tofinosecurity.com/article/tofino%E2%84%A2-enforcer%E2%84%A2-revolutionizes-modbus-tcpip-security

Tofino Modbus TCP Enforcer Loadable Security Module Information

https://www.tofinosecurity.com/products/Tofino-Modbus-TCP-Enforcer-LSM

The Data Sheet for this product follows this White Paper.

Tofino OPC Enforcer Loadable Security Module Information

http://www.tofinosecurity.com/products/Tofino-OPC-Enforcer-LSM

The Data Sheet for this product follows this White Paper.

Securing Your OPC Classic Control System

http://www.opcfoundation.org/DownloadFile.aspx?CM=3&RI=781&CN=KEY&CI=282&CU=4

Using Tofino™ to Control the Spread of Stuxnet Malware

http://www.tofinosecurity.com/professional/using-tofino-control-stuxnet

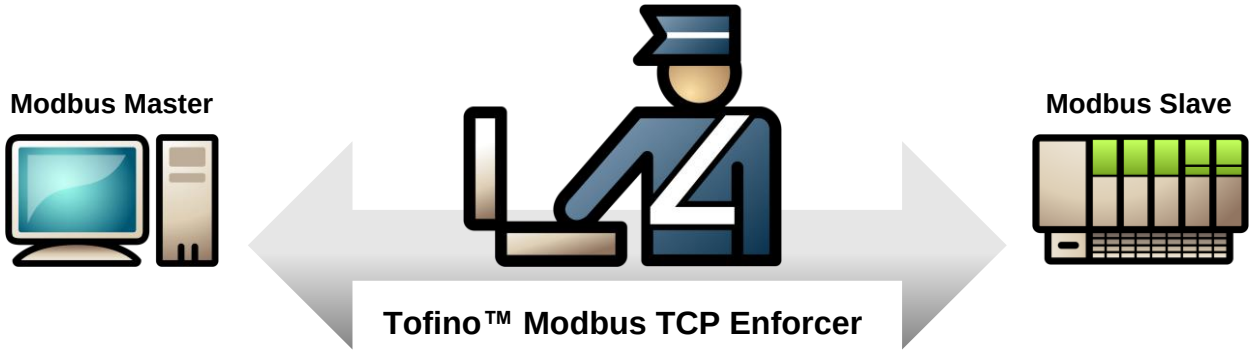
Video: MTL Instruments' security video showing how a worm on a USB key attacks a PLC over Modbus TCP

http://www.youtube.com/watch?v=G4E0bxZGZL0

Tofino™ Modbus TCP Enforcer LSM

Content Inspection for Modbus

Data Sheet
DS-MBT-LSM
Version 5.1



Advanced cyber threat and safety protection for your Modbus devices

Did you know that any device with a network connection to a Modbus controller can potentially CHANGE any of the controller's I/O points or register values? Many controllers can even be reset, disabled, or loaded with new logic or firmware.

The Tofino Modbus TCP Enforcer is a content inspector for Modbus communications, checking every Modbus command and response against a list of 'allowed' commands defined by your control engineers. Any command that is not on the 'allowed' list, or any attempt to access a register or coil that is outside the allowed range, is blocked and reported.

The Tofino Modbus TCP Enforcer makes sure that the only Modbus commands your control devices receive are approved commands from approved computers. Accidents involving remote programming are prevented and corrupted messages are blocked, making your control system safer and more reliable.

Saves you money through:

- Simplifying compliance to safety and security standards
- Reduced down time and production losses
- Lower maintenance costs
- Improved system reliability and stability

Unique capabilities:

- First-ever application of deep packet inspection technology for industrial protocols
- Control specialist defines list of allowed Modbus commands, registers and coils
- Automatically blocks and reports any traffic that does not match the rules
- Protocol 'Sanity Check' blocks any traffic not conforming to the Modbus standard
- Supports multiple master and slave devices
- Simple configuration and monitoring using the Tofino CMP
- Certified Modbus compliant by Modbus-IDA

Typical applications:

- Oil & gas custody transfer
- Safety instrumentation systems
- Managing PLC programming stations
- Display-only HMI panels
- Partner access to telemetry data

FROST & SULLIVAN
2010 World Customer Value Enhancement Award
tofinosecurity.com/awards

TOFINO®

Tofino™ Modbus TCP Enforcer LSM

Features and Specifications

Data Sheet
DS-MBT-LSM
Version 5.1

Supports multiple connections	Multiple master and slave Modbus devices are supported, with a unique set of inspection rules and options for each master/slave connection
Default filter policy	Deny by default: any Modbus function code, or register or coil address, that is not on the 'allowed' list is automatically blocked and reported
Modbus function codes	Supports functions 1-8, 11-17, 20-24, 40, 42, 43, 48, 66, 67, 91, 100, 125, 126
User-settable options	The following options may be set on a per-connection basis: ▪ Permitted Modbus function codes ▪ Permitted register or coil address range ▪ Permitted Modbus Unit IDs ▪ Sanity check enable/disable ▪ State tracking enable/disable ▪ TCP Reset on blocked traffic (when utilizing TCP transport protocol) ▪ Modbus exception reply on blocked traffic
Transport protocols	Both Modbus/TCP and Modbus/UDP supported
Configuration method	Simple configuration using the Tofino Central Management Platform (CMP)
Throughput	1000 packets per second with full content inspection
Operating modes	▪ All standard *Tofino* modes supported: ▪ *Passive*: all traffic allowed, no alerting ▪ *Test*: all traffic allowed; alerts generated as per user rules ▪ *Operational*: traffic filtered and alerts generated as per user rules
Security alerts	Reports blocked traffic to the Tofino CMP via Tofino Exception Heartbeats
Certifications	Certified Modbus compliant by Modbus-IDA
System requirements	▪ Tofino Security Appliance ▪ Tofino Firewall LSM ▪ Tofino Central Management Platform (CMP)
Ordering information	Part number: **LSM-MBT-100** Name: **Tofino™ Argon Modbus TCP Enforcer LSM** For additional information, visit www.tofinosecurity.com/buy/tofino-argon

Tofino™ Modbus TCP Enforcer LSM is a component of the Tofino Security Solution:

Tofino Security Appliance

Hardware platform that creates Plug-n-Protect™ zones of security on control and SCADA networks

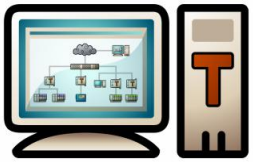
Loadable Security Modules

Firmware modules that customize the security features of each Tofino SA:

- **Firewall:** Directs and controls industrial network traffic
- **Modbus and OPC Enforcers:** Content inspection and connection management for Modbus and OPC
- **Secure Asset Management:** Tracks and identifies network devices
- **VPN:** Secures remote communication
- **Event Logger:** Reliably logs security events and alarms

Tofino CMP

Software that provides coordinated security management of all Tofino Security Appliances from one workstation or server



Your authorized Tofino supplier:

TOFINO™
tofinosecurity.com

Tofino™ OPC Enforcer LSM

Tracks and secures OPC connections

Data Sheet
DS-OPC-LSM
Version 5.0

Advanced cyber security for OPC Classic communications

OPC Classic, based on Microsoft COM/DCOM technology, is widely used in control systems as an interoperability solution, interfacing control applications from multiple vendors. But the DCOM technologies underlying OPC Classic were designed before network security issues were widely understood. As a result, OPC Classic is almost impossible to secure using a conventional firewall.

The Tofino OPC Enforcer Loadable Security Module (LSM) inspects, tracks and secures every connection that is created by an OPC application. It dynamically opens only the TCP ports that are required for each connection, and only between the specific OPC client and server that created the connection. It's simple to use – no configuration changes are required on the OPC clients and servers – and offers superior security over what can be achieved with conventional firewall or tunneler solutions.

Your OPC clients and servers are vital to the operation of your plant. Protect them now with the Tofino Security Appliance and Tofino OPC Enforcer LSM.

Saves you money through:

- Improved system reliability and stability
- Simplifying compliance to safety and security standards
- Reduced down time and production losses
- Lower maintenance costs

Unique capabilities:

- First-ever application of connection tracking technology to industrial protocols
- Secures OPC DA, HDA, or A&E
- Automatically tracks TCP ports assigned by OPC servers for data connections and dynamically opens those ports in firewall
- 'Sanity Check' blocks any OPC requests not conforming to the DCE/RPC standard
- Programmable data connection delay period to shut down unused connections
- Supports multiple OPC clients and servers
- Simple configuration and monitoring using the Tofino CMP

Typical applications:

- Manage all network traffic on systems that use OPC DA, HDA or A&E
- Secure data transfers to and from data historians and supervisory applications
- Protect safety instrumentation systems
- Combine with Tofino VPN LSM for secure remote OPC connections

FROST & SULLIVAN
2010 World Customer Value Enhancement Award
tofinosecurity.com/awards

TOFINO®

Tofino™ OPC Enforcer LSM

Features and Specifications

Data Sheet
DS-OPC-LSM
Version 5.0

Supports all variations of DCOM-based OPC	Data Access (DA), Historical Data Access (HDA), Alarms and Events (A&E), Data eXchange (DX), and XML Data Access (XML-DA)
Supports multiple connections	Multiple OPC clients and servers can be protected by a single Tofino Security Appliance running the OPC Enforcer LSM
Default filter policy	Deny by default including: ▪ Any attempted OPC traffic that is not between defined OPC client and server pairs will be blocked and reported ▪ Any attempted TCP connection that was not successfully negotiated between a valid OPC client and server will be blocked and reported
User-settable options	The following options may be set: ▪ Sanity check enable/disable on all OPC connection attempts ▪ Packet fragmentation controls ▪ Maximum time to wait for data connection to start
Configuration method	Simple configuration using the Tofino Central Management Platform (CMP)
Operating modes	All standard Tofino modes supported: ▪ Passive: all traffic allowed, no alerting ▪ Test: all traffic allowed; alerts generated as per user rules ▪ Operational: traffic filtered and alerts generated as per user rules
Security alerts	Reports security alerts to the Tofino CMP via Tofino Exception Heartbeats and via syslog (provided Event Logger LSM is installed)
Certifications	Tested for OPC protocol compliance using OPC Foundation test suite
System requirements	▪ Tofino Security Appliance ▪ Tofino Firewall LSM ▪ Tofino Central Management Platform (CMP)
Ordering information	Part number: **LSM-OPC-100** Name: **Tofino™ Argon OPC Enforcer LSM** For additional information, visit www.tofinosecurity.com/buy/tofino-argon

Tofino™ OPC Enforcer LSM is a component of the Tofino Security Solution:

Tofino Security Appliance

Hardware platform that creates Plug-n-Protect™ zones of security on control and SCADA networks

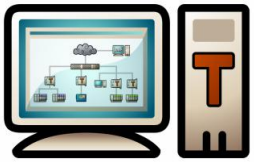
Loadable Security Modules

Firmware modules that customize the security features of each Tofino SA:

- **Firewall:** Directs and controls industrial network traffic
- **Modbus and OPC Enforcers:** Content inspection and connection management for Modbus and OPC
- **Secure Asset Management:** Tracks and identifies network devices
- **VPN:** Secures remote communication
- **Event Logger:** Reliably logs security events and alarms

Tofino CMP

Software that provides coordinated security management of all Tofino Security Appliances from one workstation or server



Your authorized Tofino supplier:

DAANET
CONTROL INFORMATION CONNECTIVITY
Ph. 1300 DAANET (1300 322 638) www.daanet.com.au

TOFINO™
tofinosecurity.com